Overview of Federal Personnel Vetting

Student Guide

March 2025

Center for Development of Security Excellence

Contents

Lesson 1: Course Introduction

Introduction

Introduction

Welcome to your Overview of Federal Personnel Vetting. Through this course, you will be introduced to the laws, goals, and processes for this vital government function.

Federal Personnel Vetting (FPV) is the process in which trusted government personnel effectively manage risk by evaluating reliable and relevant information from background investigations and other reliable sources to make trust determinations or adjudicative decisions for suitability, fitness, national security, and credentialing.

By following the policies and procedures laid out in this course, you will work to ensure the people, property, information, and mission of United States government agencies are secure.

About This Course

To explore the FPV program, in this course you will follow a hypothetical scenario. The Department of Defense (DOD) is constructing a new office complex, which it will need to staff with trusted insiders with access to classified information. You will follow several candidates for this new team as their information is collected by investigative service providers and as adjudicators determine whether each candidate may pose a risk to national security.

Take a moment to review the course objectives before you begin.

- Given a description, determine the governing documents and principles related to the Federal Personnel Vetting Program and judicial cases and practices that have influenced the personnel vetting process.
- Given a description, determine the Federal Personnel Vetting Policy Framework and procedures for making trust determinations.

Lesson 2: Governing Authorities and Judicial Cases

Introduction

Lesson Introduction

The Federal Personnel Vetting (FPV) program is a vital part of our national defense, responsible for protecting our Federal workforce. It is an essential government function, and it must follow the blueprints created by the Federal government. This includes laws passed by Congress, regulations, Executive Orders, and directives by the Executive branch, and court cases and other actions by the Judicial branch. Together, these laws and actions form the framework of the FPV program. In this lesson, you will explore the laws, policies, and judgments that have made the FPV program what it is today.

Take a moment to review the lesson objectives:

- Interpret applicable U.S. laws, E.O.s, SEADs, ICDs, ICPG, and national policies governing the Federal Personnel Vetting process.
- Interpret the Freedom of Information and Privacy Acts and other Federal laws, policies, and regulations that ensure privacy and civil liberties.
- Describe how past events have impacted national security and shaped personnel vetting.
- Explain how SEAD 9 ensures compliance with whistleblower protection statutes.

Laws and Congressional Actions

History of Federal Personnel Vetting

Much of the outline of the FPV program is formed by laws written and passed by Congress. To keep pace with our changing world and technological progress, laws must be written to give the program new capabilities and responsibilities. You should be familiar with the history of these laws and congressional actions, which form the foundation of the FPV program.

National Security Act of 1947

- Title VII establishes requirements for accessing classified information, including background checks and uniform standards.

Privacy Act of 1974

- The Privacy Act states agencies must maintain accurate and complete records and protect them from unauthorized use
- It allows individuals to access their own personnel records
- Some exempted information may still be withheld for national security or law enforcement reasons

Intelligence Reform and Terrorism Prevention Act of 2004

- The Intelligence Reform and Terrorism Prevention Act requires a single department or agency to be responsible for security clearances and investigations
- It requires all agencies to reciprocally accept background investigations and determinations made by other agencies
- The Act establishes the requirement for an Information Sharing Environment for sharing terrorism information across agencies

50 USC § 3234

- Part of the Intelligence Reform and Terrorism Prevention Act, this law prohibits the FPV program from retaliating against employees and candidates who are lawful whistleblowers

50 USC § 3341

- Part of the Intelligence Reform and Terrorism Prevention Act, this law establishes a single agency responsible for directing investigations and adjudications
- It establishes the principle of reciprocity and the database on security clearances

Freedom of Information Act (FOIA)

- The Freedom of Information Act allows individuals to request records from Federal agencies, including some types of background checks and processes

- Personnel files are generally exempted from FOIA requests to protect individual privacy
- Exemptions for national security and law enforcement purposes may also apply

Knowledge Check 1

Frances, a Federal employee with access to Secret-level information, recently filed a lawful whistleblower complaint relating to work performed in her office. Now she is being vetted for access to Top Secret information. How does 50 USC § 3234 impact her case?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Frances's trust determination may not be denied on the basis of her complaint.
- ○ Information about Frances's whistleblower action is exempted from FOIA requests.
- ○ Lawful whistleblowers must not have access to Top Secret information.
- ○ Frances must be granted Top Secret clearance by default.

Knowledge Check 2

Walter is being vetted for a role accessing Secret information. How does the Privacy Act of 1974 impact his case?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Walter has waived all privacy rights during the vetting process.
- ○ It allows Walter to access his own personnel records, unless information is exempted for national security reasons.
- ○ Walter is prohibited from becoming a whistleblower.
- ○ Walter's information may not be stored in a secure database.

Executive Actions

Federal Regulations

To enforce the laws passed by Congress, the FPV program uses many regulations published in the Code of Federal Regulations (CFRs).

5 CFR Part 731 – Suitability and Fitness

- This regulation establishes investigation, continuous vetting, and reciprocity requirements for Suitability, and position designation requirements, investigative standards, and reciprocity requirements for Fitness.
- It establishes the criteria and procedures for making suitability determinations and taking suitability actions in cases involving covered positions that are subject to investigation

5 CFR Part 732 – National Security Positions

- This regulation establishes National Security investigation and adjudication requirements and procedures

5 CFR Part 1400 – Designation of National Security Positions

- This regulation establishes National Security position designations and investigation requirements
- It clarifies the requirements and procedures that agencies should observe when designating *national security* positions, including
  - Positions in the competitive service
  - Positions in the excepted service where the incumbent can be noncompetitively converted to the competitive service
  - Senior Executive Service (SES) positions held by career appointees in the SES within the Executive Branch

32 CFR Part 117 – National Industrial Security Program Operating Manual (NISPOM)

- This regulation establishes security requirements for cleared contractors operating under the National Industrial Security Program (NISP)
- It describes how the FPV program is applied to contractors with access to classified information

Presidential Issuances

In addition to regulations by departments and agencies, the President of the United States can issue Executive Orders (E.O.s) and other directives to provide instructions to federal agencies.

Presidential Policy Directive (PPD) 19: Protecting Whistleblowers with Access to Classified Information

- This directive establishes requirements to ensure that members of the Intelligence Community (IC) or who are eligible for access to classified information can effectively report waste, fraud, and abuse while protecting classified national security information

E.O. 10450: Security Requirements for Government Employment

- This Executive Order requires that all persons who are employed by the departments and agencies of the government shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States, and that retention be clearly consistent with the interests of the national security
- It also requires that the scope of investigations be determined by the degree of adverse effect the occupant of the position could bring to the national security
- It requires positions that could bring a material adverse effect on national security to be designated as sensitive positions.

E.O. 10865, as amended: Safeguarding Classified Information within Industry

- This Executive Order establishes appeal rights and procedures for industry applicants determined ineligible for access to classified information

E.O. 12333, as amended: United States Intelligence Activities

- This Executive Order establishes the Executive Branch’s framework for our national intelligence efforts and for protecting privacy and civil liberties in the conduct of intelligence activities

E.O. 12968, as amended: Access to Classified Information

- This Executive Order establishes the uniform Personnel Security Program (PSP) for employees who are considered for initial or continued access to classified information
- It also establishes security policies designed to protect classified information

E.O. 13467, as amended: Reforming Processes Related to suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information

- This Executive Order establishes policy and procedures for vetting individuals who work for or on behalf of the Federal Government
- It establishes the role of Security Executive Agent (SecEA) to oversee the requirements for national security eligibility and designated the Director of National Intelligence (DNI) to fill the role to align background investigations and adjudications and maximize consistency and efficiency

E.O. 13488, as amended: Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust

- This Executive Order addresses reciprocity and reinvestigations for public trust positions

E.O. 13764: Amending the Civil Service Rules, Executive Order 13488, and Executive Order 13467 to Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters

- This order amends and updates E.O.s 13467 and 13488 with the goal of modernizing the governing structure of the FPV program
- It updates the processes for security clearances, suitability and fitness for employment, and credentialing and related matters
- It also prescribes reciprocity, continuous evaluation, and process improvements using enterprise-wide capabilities

E.O. 13869: Transferring Responsibility for Background Investigations to the Department of Defense

- This Executive Order transferred the investigative functions of the National Background Investigations Bureau to the Defense Counterintelligence and Security Agency (DCSA) within the DOD

Security Executive Agent Directives (SEADs)

In their role as the Security Executive Agent (SecEA), the Director of National Intelligence (DNI) has issued nine Security Executive Agent Directives (SEADs) defining the policy and procedures of the FPV program.

SEAD 1: Security Executive Agent Authorities and Responsibilities

- SEAD 1 consolidates and summarizes the authorities and responsibilities of the SecEA to develop, implement, and oversee policies and procedures governing the conduct of investigations and adjudications for eligibility for access to classified information or eligibility to hold a sensitive position

SEAD 2: Use of Polygraph in Support of Personnel Security Determinations for Initial or Continued Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position

- SEAD 2 establishes policy and assigns responsibilities governing the use of polygraph examinations conducted by agencies in support of personnel security vetting for initial or continued eligibility for access to classified information, or eligibility to hold a sensitive position
- Polygraph examination types include Counterintelligence Scope Polygraphs (CSP), Expanded Scope Polygraphs (ESP), and Specific Issue Polygraphs (SIP)

SEAD 3: Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position

- SEAD 3 establishes reporting requirements for all covered individuals who have access to classified information or hold a sensitive position

- This directive does not limit the authority of agency heads to impose additional reporting requirements in accordance with their respective authorities under law or regulation

SEAD 4: National Security Adjudicative Guidelines

- SEAD 4 establishes the single, common adjudicative criteria for all covered individuals who require initial or continued eligibility for access to classified information or eligibility to hold a sensitive position

SEAD 5: Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications

- SEAD 5 provides guidance for the collection, use, and retention of publicly available social media information for initial and continued eligibility for access to classified information or to hold a sensitive position

SEAD 6: Continuous Evaluation (CE)

- SEAD 6 establishes policy and requirements for the continuous evaluation of individuals who require eligibility for access to classified information or to occupy a national security position

SEAD 7: Reciprocity of Background Investigations and National Security Adjudications

- SEAD 7 establishes requirements for reciprocal acceptance of background investigations and national security adjudications for initial or continued eligibility for access to classified information or eligibility to hold a sensitive position

SEAD 8: Temporary Eligibility

- SEAD 8 establishes policy and requirements for authorizing temporary eligibility for access to classified information or temporary eligibility to occupy a sensitive position, or to a higher level

SEAD 9: Whistleblower Protection: Appellate Review of Retaliation Regarding Security Clearances and Access Determinations

- SEAD 9 establishes policy for the Director of National Intelligence's appellate review process for employees who seek to appeal an adverse final agency determination with respect to alleged retaliatory actions taken by an employing agency affecting the employer's security clearance or access determination as a result of protected disclosures

ICDs and ICPGs

In addition to SEADs, the Director of National Intelligence (DNI) may issue Intelligence Community Directives (ICDs) and Intelligence Community Policy Guidance (ICPGs) to provide additional policy and procedures for the Intelligence Community and other federal employees with access to classified information. ICDs are used to set high-level policy, while ICPGs provide more specific instructions to meet the goals of the ICDs.

ICD 704: Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information

- ICD 704 directs the implementation of the PSP within the Intelligence Community (IC)
- It lays out policy and procedures for access to Sensitive Compartmented Information (SCI), establishes baseline personnel security standards and exceptions for access to SCI, and authorizes polygraph programs for IC elements

ICPG 704.1: Personnel Security Investigative Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information

- ICPG 704.1 expands on ICD 704 by
    - Providing investigative standards for access to SCI and controlled access programs
    - Setting policy for source collection
    - Establishing investigative standards, including coverage, estimates, and time periods

- Establishing requirements for training and quality control

ICPG 704.3: Denial or Revocation of Access to Sensitive Compartmented Information, Other Controlled Access Program Information, and Appeals Processes

- ICPG 704.3 mandates that individuals who have been considered for and denied initial or continued access to SCI shall be afforded an opportunity to appeal
- It establishes a process for all appeals

ICPG 704.4: Reciprocity of Personnel Security Clearance and Access Determinations

- ICPG 704.4 provides guidance on the application of reciprocity in accordance with SEAD 7, including situations where adjudicative decisions differ between agencies
- It establishes the SecEA as the final arbitrative authority between agencies regarding adjudications
- It also mandates standardized training for investigative and adjudicative personnel

ICPG 704.5: Intelligence Community Personnel Security Database Scattered Castles

- ICPG 704.5 establishes Scattered Castles as the repository for all clearance and access determinations
- It defines roles and responsibilities to operate and support Scattered Castles

ICPG 704.6: Conduct of Polygraph Examinations for Personnel Security Vetting

- ICPG 704.6 provides guidance for authorizing and conducting polygraph examinations
- It distinguishes policy and requirements for CSPs, ESPs, and SIPs

Knowledge Check 3

Miranda is an information security specialist transferring to a new agency within the DOD. How does Executive Order 13488 apply to her case?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ E.O. 13488 requires Miranda's new agency to reciprocally accept her previous trust determination.
- ○ E.O. 13488 limits Miranda's mobility in transferring between agencies.
- ○ E.O. 13488 requires Miranda to undergo a new investigation.
- ○ E.O. 13488 limits which parts of Miranda's record are stored in Scattered Castles.

Knowledge Check 4

Zay is transferring from a cleared position with Army Medical Research to a task force dealing with biological weapons. He is denied an upgraded security clearance, and he believes it is retaliation for a lawful whistleblower complaint he made in a previous position. How does SEAD 9 apply to his case?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ SEAD 9 states that denials of security clearance are final, regardless of the reason.
- ○ SEAD 9 establishes a process to appeal the decision.
- ○ SEAD 9 prohibits any appeal for positions involving weapons of mass destruction.
- ○ SEAD 9 gives Zay a right to review his investigation file for evidence of retaliation.

Judicial Precedents and High-Profile Events

Judicial Precedents

Actions by the Judicial Branch ensure that the FPV program complies with the requirements of the United States Constitution and other Federal laws. Over the years, many court decisions have shaped the PSP and FPV programs, both by limiting its scope to protect the civil rights of U.S. citizens and by upholding the importance of the program.

Decisions Limiting Scope

In Cole vs. Young, the Supreme Court limited the PSP to the regulation of sensitive positions only.

In Service vs. Dulles, the Supreme Court asserted that an agency must follow its own regulations, even when those regulations are more restrictive than the law requires.

In Greene vs. McElroy, the Supreme Court established due process procedures for the PSP.

Decisions Upholding Mission

In Adams vs. Laird, the judges affirmed the right of the PSP to deny or revoke a national security eligibility because of questions about a subject's loyalty, trustworthiness, and reliability. Decisions are discretionary and do not need to adhere to an evidentiary standard.

In Clifford vs Shoultz, the judges ruled that the investigative process is not equivalent to a trial, and individuals do not have a right to avoid self-incrimination. An individual's refusal to provide information may be grounds for an unfavorable security determination.

In United States vs. Yermian, the judges stated that the willful falsification of information is cause for the denial of a national security eligibility, even if the falsifier did not specifically intend to deceive the government.

In Department of the Navy vs. Egan, the Supreme Court stated that national security eligibility is a judgment call and "may be granted only when 'clearly consistent with the interests of the national security.'" Any doubt concerning personnel being considered for national security eligibility will be resolved in favor of the national security over the individual.

High-Profile Events

Many of the latest reforms to the FPV program, including the modern continuous vetting program, were spurred by attacks on national security from both insiders and adversaries overseas.

In July 2013, Chelsea Manning, an Army servicemember, was convicted for transmitting hundreds of thousands of classified documents to the website Wikileaks. Manning had access to Top Secret information and SCI.

On September 16, 2013, Aaron Alexis, a cleared contractor and former Navy servicemember, smuggled a firearm into the Washington Navy Yard in Washington,

D.C., where he killed 12 people and injured three others. Alexis had been granted Secret-level eligibility in spite of previous arrests involving a firearm.

In 2014, OPM was the target of two data breaches, possibly conducted by state-sponsored attackers in China. The attack resulted in the loss of millions of employment and background investigation records. The attack was made more serious because aging cybersecurity tools prevented discovery of the attacks for many months. Partly because of these breaches, the government created DCSA to oversee personnel vetting and introduced new policies to promote information security.

Knowledge Check 5

According to Clifford vs. Shoultz, because a background investigation is not a trial:

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Adjudicators must prove an individual is a risk to national security.
- ○ Individuals are not required to swear that their responses are true.
- ○ Agencies are not required to maintain strict records.
- ○ Individuals may be denied security clearance for their refusal to answer questions.

Knowledge Check 6

What is one way the FPV program has changed in response to events like the OPM Data breaches?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Individuals must be given an opportunity to appeal a denial of security clearance.
- ○ Security clearance may only be denied when it is consistent with the national interest.
- ○ DCSA was created to oversee personnel vetting, and new policies to promote information security were introduced.
- ○ The FPV program has not changed in response to these events.

Lesson Conclusion

Lesson Summary

You have completed the *Governing Authorities and Judicial Cases* lesson.

Lesson 3: Federal Personnel Vetting Policy

Introduction

Lesson Introduction

Now that you have learned about the laws and regulations that govern the Federal Personnel Vetting (FPV) program, it's time to take a closer look at the policies that form its foundation and detail how the program is carried out, including core doctrine, guidelines, and investigative standards.

Remember the hypothetical new DOD office? As applicants to that new office move through the vetting process, we will observe how these foundational FPV policies describe the goals, principles, processes, and techniques that make the program work.

Review the lesson objectives before continuing on.

- Determine the purpose of the Federal Personnel Vetting Policy Framework and program.
- Describe the Federal Personnel Vetting Guidelines and Standards.

FPV Purpose and Framework

The TW 2.0 Framework

The FPV program is in a period of transition. The Security, Suitability, and Credentialing Performance Accountability Council (PAC) is spearheading program reforms under the Trusted Workforce 2.0 (TW 2.0) initiative. Together, the Security Executive Agent (SecEA) and Suitability and Credentialing Executive Agent (Suit/Cred EA) provide leadership for the program. The goal of these reforms is to better support agencies' missions by reducing the time required to bring new hires onboard, enabling mobility of the Federal workforce, and improving insight into workforce behaviors.

The TW 2.0 Framework consists of one Personnel Vetting Policy Framework that aligns vetting processes with a simplified framework of Executive issuances,

guidelines, and standards; three investigative tiers to accelerate processing times, reduce duplication and complexity, and improve mobility; and five vetting scenarios to follow the lifecycle of an individual working for or on behalf of the Federal Government.

You will learn more about the tiers and scenarios in the next lesson.

FPV Policy Organization

To accomplish its goal of ensuring a vetted and secure workforce, the FPV program is supported by a suite of policies organized in a top-down hierarchical structure with four levels, where each level is more agile than the one before.

At the top is the strategic level, consisting of the TW 2.0 Federal Personnel Vetting Core Doctrine and Executive Correspondence.

Next is the Guidelines level of policies, including the FPV Guidelines, which describe outcomes of a successful vetting program.

Beneath that are the Operational level policies, like the Investigative Standards, that are oriented toward compliance and include tools like standards, principles, and common forms.

The last level is Tactical and includes appendices and forms that are applied in the personnel vetting mission's set of duties.

Federal Personnel Vetting Core Doctrine

The Federal Personnel Vetting Core Doctrine provides top-level strategic guidance for transformative reforms to the FPV program and processes. It establishes the government's FPV philosophy and defines its mission, guiding principles, key supporting processes, and policy priorities.

The Core Doctrine aligns FPV processes together, promotes mobility, improves efficiencies, and moves the program forward toward an enhanced risk management approach.

Federal Personnel Vetting Guidelines

Issued by the SecEA and Suit/Cred EA together, in alignment with the Core Doctrine, the Federal Personnel Vetting Guidelines define the intended outcomes of the FPV program, including outcomes for investigations, adjudications, and personnel vetting management practices. They describe the essential components for identifying and managing human risk to ensure the Federal workforce is a trusted workforce.

Janelle is an applicant to the new DoD office. The Guidelines detail the high-level outcomes for the FPV risk management framework, including how Janelle will be assessed against the characteristics of a trusted person. The Guidelines also detail the successful outcomes for the five personnel vetting scenarios and the central elements of the FPV program.

Federal Personnel Vetting Investigative Standards

In May, 2022, the SecEA and Suit/Cred EA issued new Federal Personnel Vetting Investigative Standards. Their goal is to implement a risk management approach to background investigations that maximizes uniformity across all FPV domains and focuses on the efficient collection of information needed to make informed trust determinations.

Where the previous Standards emphasized obtaining specific numbers of each type of information source, the new Standards emphasize obtaining the most relevant sources of information. The Standards also bring investigative trigger thresholds in line with today's current realities, tailoring the required expansion toward the specific information needed to resolve any underlying issues.

The Investigative Standards guide background investigators to collect information that aligns with the adjudicative criteria for each type of trust determination. The factors for Suitability in 5 CFR Part 731, for Fitness, which are determined by the hiring agency, Guidelines for National Security Eligibility, which are defined in SEAD 4, and standards for Credentialing, in Homeland Security Presidential Directive (HSPD-12) provide templates for what a trusted person looks like. The FPV Investigative Standards describe the information needed to evaluate candidates against that template.

Case File: Glen Lantagne

Let's explore an example of how the Investigative Standards allow the FPV program to meet its Guidelines. Glen has applied to our new DOD facility. He is being vetted for his suitability to hold his first Federal position. The FPV program's investigative model is aligned to attributes and information types that can show whether Glen can be a trusted person, whether he demonstrates a regard for rules, appropriately engages others, demonstrates conduct consistent with the interests of the United States, and demonstrates a willingness and ability to protect people, property, information, and mission.

To accomplish this, the Investigative Standards guide the collection of information in 16 categories:

- Citizenship and legal status

- Criminal history
- Education history
- Employment and military history
- Financial history
- Foreign activities and associations
- Handling of protected information or systems
- Identity resolution
- Interpersonal engagement
- Investigative and adjudicative records
- Non-criminal public records
- Publicly available electronic information
- Psychological considerations
- Self-provided information
- Substance misuse or abuse
- Violent extremist, terrorist, and unlawful subversive actions

Using this information, the adjudicator can make an informed determination for each individual.

Comparison

As you just learned, the FPV program is founded on many crucial documents. In this lesson you were introduced to the Core Doctrine, Guidelines, and Investigative Standards.

Remember, the FPV Core Doctrine provides the philosophy, goals, and priorities for all PV policy.

The FPV Guidelines are derived from the Core Doctrine and apply its principles to provide the high-level direction, outcomes, and essential components of the program.

The FPV Investigative Standards provide specific guidance and procedures for background investigators to collect sufficient information to meet the requirements of the FPV program.

Knowledge Check 1

Which of the following statements correctly describes the Federal Personnel Vetting Core Doctrine?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ This document provides the philosophy for and guides all FPV policy.
- ○ This document defines intended outcomes for the FPV program, including investigations, adjudications, and PV management.
- ○ This document provides specific procedures for background investigations.

Knowledge Check 2

Which of the following statements correctly describes the Federal Personnel Vetting Guidelines?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ This document provides the philosophy for and guides all FPV policy.
- ○ This document defines intended outcomes for the FPV program, including investigations, adjudications, and PV management.
- ○ This document provides specific procedures for background investigations.

Knowledge Check 3

Which of the following statements correctly describes the Federal Personnel Vetting Investigative Standards?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ This document provides the philosophy for and guides all FPV policy.
- ○ This document defines intended outcomes for the FPV program, including investigations, adjudications, and PV management.
- ○ This document provides specific procedures for background investigations.

Lesson Conclusion

Lesson Summary

You have completed the Federal Personnel Vetting Policy lesson.

Lesson 4: Federal Personnel Vetting Program Framework

Introduction

Lesson Introduction

The new offices for the Department of Defense (DOD) are coming together, and candidates are applying to open positions. Before you can properly vet them, you will need to see how the Federal Personnel Vetting (FPV) program is organized.

In this lesson you will learn how the one personnel vetting framework, three investigative tiers, and five vetting scenarios you were introduced to in the previous lesson are applied to personnel vetting across all four vetting domains, ensuring every potential insider receives exactly the vetting they need.

Review the lesson objectives before continuing on.

- Explain the personnel vetting domains.
- Explain the three-tier investigative framework of the FPV investigative standards, five FPV scenarios, and the associated requirements.
- Explain national security position designations and special access requirements.

Personnel Vetting Domains

The Four Domains

FPV is how individuals undergo investigation, evaluation, adjudication and continuous vetting to determine whether they are now – and are likely to remain – loyal, trustworthy, and reliable insiders. FPV is organized into four domains—Suitability, Fitness, National Security, and Credentialing—that describe the traits and characteristics required for different position requirements and types of access.

Suitability

Daphne has applied to be an information security professional at the new office. Before she can take the position, DOD must first decide whether she is suitable for employment.

Suitability is the sum of all the character traits and conduct that indicate Daphne could carry out the duties of a Federal position with integrity, efficiency, and

effectiveness. In other words, could her character or conduct have an adverse impact on the integrity or efficiency of the service?

During the investigation process, Investigative Service Providers (ISPs) will collect information relating to each of the factors found in 5 Code of Federal Regulations (CFR) Part 731, which provides the standards for suitability.

After her information is collected and compiled into a report of investigation, adjudicators will evaluate it and make a suitability trust determination for Daphne.

Fitness

Cole has applied to be a contracted data analyst on a project at the new office. Because he is not applying for a competitive Federal position, his first trust determination will involve Fitness rather than Suitability.

Fitness determinations are applied to excepted service positions, Non-Appropriated Fund (NAF) positions, and contracted positions. Criteria for the determination are identified by the agency and tailored to the specific position. ISPs collect that information, which adjudicators will evaluate to make a Fitness trust determination.

National Security Eligibility

Chris has applied to be an inventory manager at the new office. This is a sensitive position that requires eligibility for access to classified information.

National security adjudication seeks reasonable assurance that Chris will be loyal, trustworthy, and reliable in his handling of classified information. These determinations are stringent, taking into account his entire personality and character: his stability, trustworthiness, reliability, discretion, honesty, and judgment.

During the investigation, the ISP will collect information relating to the guidelines in SEAD 4, and the adjudicator will evaluate it to make a national security trust determination.

Suppose the adjudicator makes an unfavorable determination in Chris's case. It's important to note the adjudicator's responsibilities in making and documenting these determinations. This means ensuring the adjudicative records are accurate, relevant, timely, and complete to the extent reasonably necessary; complying with all applicable administrative due process requirements; providing Chris at a minimum with notice of the specific reasons for the decision, an opportunity to respond, and notice of appeal rights, if he has any; considering all

available information in reaching their final decision; and keeping any record of the agency action required by OPM as published in its issuances.

Credentialing

Stella is applying to be a security professional in the new office. She will need a credential to gain physical access to the building and logical access to its information systems.

Credentialing, also known as the Homeland Security Presidential Directive (HSPD) 12 adjudication, determines who may receive a Personal Identity Verification (PIV) credential. In the DOD the PIV is known as a Common Access Card (CAC).

Stella's credentialing determination aims to ensure that she is not a known or suspected terrorist, does not provide an avenue for terrorism at Federal facilities, and does not pose an unacceptable risk to Federal employees or assets.

During the investigation, ISPs will collect information relating to the criteria in HSPD-12, and the adjudicator will evaluate this information to make a credentialing trust determination.

Knowledge Check 1

The new team will hire an Information Systems Manager who requires Top Secret eligibility and access. Determining whether the individual has the trustworthiness to meet that requirement falls under which domain?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Suitability
- ○ Fitness
- ○ National Security
- ○ Credentialing

Knowledge Check 2

The new team will hire a Program Analyst, who will be a Federal employee. Determining whether the individual has the character and conduct necessary for that position falls under which domain?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Suitability

- ○ Fitness
- ○ National Security
- ○ Credentialing

Knowledge Check 3

The new team will hire an Administrative Assistant to support the daily activity of the office. Determining whether the individual is a risk to Federal facilities and information systems falls under which domain?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Suitability
- ○ Fitness
- ○ National Security
- ○ Credentialing

Three Tiers and Five Scenarios

The Three Tiers

To support the reforms of the Trusted Workforce 2.0 initiative, the newly updated Investigative Standards establish a system of tiers and scenarios that further define the investigative requirements for each individual.

The new three-tier investigative model replaces the previous five-tier model. These tiers—High Tier, Moderate Tier, and Low Tier—reflect the vetting requirements for different positions based on the level of risk to the service and potential damage to national security.

The three tiers provide several benefits over the previous model. They enable greater workforce mobility and eliminate complexities and inefficiencies in the investigative process. Together with the five personnel vetting scenarios we will address later, these tiers align the investigative requirements for decisions in all FPV domains.

The model is built from the bottom up, starting with information requirements for all adjudication decisions in all positions. Each investigative tier builds on the one below it, with a mix of information categories and data sources that vary in complexity, coverage, and methodology as needed for each tier.

Low Tier (LT)

Clara is a graphic design specialist who is being vetted for a position supporting various elements around the office. This is a non-sensitive, low-risk position in which she will not have access to classified information. Clara will, however, need access to the facility and its computer systems.

Low Tier (LT) is the minimum investigative tier. It applies to non-sensitive, low-risk positions like Clara's, and is used to make credentialing, or HSPD-12, determinations to grant physical and logical access.

Clara will need an LT investigation.

Moderate Tier (MT)

Bo has applied for a position as a communications specialist. He will have access to Secret information.

Moderate Tier (MT) is used for Non-Sensitive, Moderate-Risk or Non-Critical-Sensitive, Moderate-Risk Public Trust positions like Bo's. This is the investigative tier necessary for eligibility and access to Confidential or Secret information, as well as L access.

Bo will need an MT investigation.

High Tier (HT)

Naomi is being vetted for a position as an intelligence analyst handling important national security information. She will require access to Top Secret information.

High Tier (HT) is used for Non-Sensitive / High Risk Public Trust positions, Non-Critical Sensitive / High-Risk Public Trust positions, Critical Sensitive / High-Risk Public Trust positions, and Special Sensitive / High-Risk Public Trust positions. These are positions with eligibility and access to Top Secret information, Sensitive Compartmented Information (SCI), or Q access.

Naomi will need an HT investigation.

The Five Scenarios

Individuals undergoing vetting will also have different investigative requirements based on their vetting scenario and the investigative tier that aligns with their position designation. As defined by the FPV Guidelines, all personnel vetting falls within one of five personnel vetting scenarios—Initial Vetting, Continuous Vetting, Upgrades, Transfer of Trust, and Re-establishment of Trust—that guide what information is collected and evaluated to make a trust determination.

The new Federal Personnel Vetting Investigative Standards outline the investigative requirements for each tier and apply them to all five vetting scenarios, based on mission needs, position designation, and an individual's relevant personal history information.

Initial Vetting

Suzanne is being vetted for her first Federal position. Through Initial Vetting, the federal government *establishes trust* with individuals like Suzanne as they are assigned to their first positions of trust. The federal government will assess whether Suzanne can be trusted to protect people, property, information, and mission.

As you learned earlier, the complexity of the investigation is based on the investigative tier for the position designation. The hiring department or agency must ensure the position has a risk and sensitivity designation, which establishes the tier. We will discuss position designations a little later in this lesson. Initial Vetting is the foundation for Continuous Vetting. The information gleaned about Suzanne at this stage provides insight and will be used as a baseline for her later ongoing vetting.

Continuous Vetting

Once Suzanne receives the preliminary or final determination from her Initial Vetting, her hiring department or agency will enroll her into Continuous Vetting. Continuous Vetting assesses risk in near real-time to provide insights into the behaviors of trusted insiders.

All individuals who have a current trust determination and need vetting to maintain access are enrolled into Continuous Vetting. The ongoing process uses automated data source checks and investigative activities at intervals determined by the investigative tier. This allows the Federal Government to maintain confidence that Suzanne will remain a trusted insider.

Upgrades

Gabriel is currently a program analyst with access to Secret information. He first underwent his Initial Vetting several years ago, and since then has been enrolled in Continuous Vetting. Now he is receiving a promotion to program manager, a role with access to Top Secret information, so Gabriel will require an Upgrade.

Upgrades quickly raise the level of vetting when an individual requires a higher level of trust within the same agency. They're used for individuals like Gabriel who are changing positions or assuming responsibilities at a higher tier than their

existing trust determination. Now that he is moving to a new position requiring a higher-level investigation, Gabriel will only receive the level of additional vetting required for the new tier, not a full vetting.

Transfer of Trust

Gerard is transferring to the new office from another agency, where he underwent his Initial Vetting and has been enrolled in Continuous Vetting. His Transfer of Trust to the new agency is based on the principle of *reciprocity*.

Reciprocity is the new agency's acknowledgement or acceptance of a previous background investigation or continuous vetting activities by an authorized investigative service provider, and/or a suitability, fitness, national security or credentialing trust determination made by an authorized adjudicative Department or Agency.

Reciprocity streamlines the movement of trusted individuals between agencies and organizations. This could include:

- A Federal employee or contractor moving to a new department or agency
- A Federal employee or contractor moving to a new component within the same department or agency
- A Federal employee becoming a contractor, or vice versa
- A contractor moving from one contract company to another, even if they are sponsored by the same agency
- If the sponsoring agency of either the contractor or their company changes

According to the principle of reciprocity, the new agency *must* accept Gerard's previous determination from the first agency, so long as it is for the same domain of trust determination and at the appropriate level for the new position.

Re-establishment of Trust

Brianna is returning to the DOD after several years in consulting. She has not had active security clearance since she left the DOD. Re-establishment of Trust simplifies her reentry back into the Federal workforce. This scenario is used for former trusted insiders like Brianna who stop working for or on behalf of the Federal Government for a time, and then seek to return.

The degree of personnel vetting required should be tailored to address the new position designation, the length of time the individual was not affiliated with the Government, and the individual's prior personnel vetting record. The goal of Re-

establishment of Trust is to eliminate any redundant personnel vetting actions and remove impediments to the re-entry and onboarding of former trusted insiders like Brianna.

Knowledge Check 4

Norris has received a promotion from Project Analyst, a Low Tier position, to Project Manager, where he will require national security eligibility at the Secret level, which requires a Moderate Tier investigation. What scenario does this fall under?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Initial Vetting
- ○ Continuous Vetting
- ○ Upgrades
- ○ Transfer of Trust
- ○ Re-establishment of Trust

Knowledge Check 5

Jonathan previously had access to Secret information, before leaving the Federal workforce to care for a sick family member. He is now returning to a national security position with the same investigative tier. What scenario does this fall under?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Initial Vetting
- ○ Continuous Vetting
- ○ Upgrades
- ○ Transfer of Trust
- ○ Re-establishment of Trust

Knowledge Check 6

Rosemary is a cleared contractor employee with access to Top Secret information. She is being vetted for a Federal position with the same level of access. What scenario does this fall under?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Initial Vetting

- Continuous Vetting
- Upgrades
- Transfer of Trust
- Re-establishment of Trust

Knowledge Check 7

Cosa received his Initial Vetting last year, and now receives periodic and automated checks. What scenario does this fall under?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- Initial Vetting
- Continuous Vetting
- Upgrades
- Transfer of Trust
- Re-establishment of Trust

Knowledge Check 8

Stephanie is an engineer who is being vetted for her first Federal contractor position. She has not worked for or on behalf of the Federal government before. What scenario does this fall under?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- Initial Vetting
- Continuous Vetting
- Upgrades
- Transfer of Trust
- Re-establishment of Trust

Position Designations

Introducing Position Designations

So far you have seen several of the positions the new office is hiring to. Each of these positions requires a position designation. The Position Designation System (PDS) is how Position Designations (PDs) are assigned in the FPV program. PDs characterize the potentially adverse impact a position may have on national security and the public's trust. The PDS assesses the duties and responsibilities of a position

to determine the associated risk and sensitivity level, and thus the necessary investigative tier.

The *risk level* of a position describes its degree of the potential adverse impact to the efficiency or integrity of the service from a candidate who is unsuitable. Risk levels can be rated Low, Moderate, or High. The *sensitivity level* shows how a position's duties present the potential to bring about a material adverse effect on national security, and how serious that damage could be. This is how the PDS ensures a systematic, dependable, and uniform way of making position risk and sensitivity designations for all positions, whether military, civilian, or contractor, in accordance with 5 CFR Parts 731 and 1400.

This system is essential to the Federal Government's effort to standardize investigation requests and allow agencies to reciprocally accept transfers of trust.

Sensitivity Levels

National security positions, as outlined in 5 CFR Part 1400, must be evaluated for a position sensitivity designation. National security positions are designated to one of three sensitivity levels, based on the degree of potential damage to national security. These levels are Special Sensitive, Critical-Sensitive, or Non-Critical Sensitive. Non-National Security positions are designated Non-Sensitive. Finally, many Special Programs require additional investigation. As a national security position's level of authority and responsibility increases, the character and conduct of individuals holding those positions become more significant.

Special-Sensitive

Wendy is being vetted for a position supervising several intelligence analysts on projects that could include Sensitive Compartmented Information (SCI). Special-Sensitive positions like hers have the potential to cause inestimable damage to national security or adversely impact the efficiency of the DOD or military services.

In accordance with 5 CFR Part 1400, Special-Sensitive positions automatically carry a High-Risk designation under 5 CFR Part 731. These include:

- Positions requiring eligibility for access to SCI or other intelligence-related Special-Sensitive information, or involvement in Top Secret Special Access Programs (SAPs)

- Positions involving independent duties or responsibilities for protecting critical infrastructure and key resources (CIKR), against acts of terrorism, espionage, or foreign aggression
- Positions with independent responsibility for identity vetting and/or unrestricted access to materials for producing credentials and badges, the compromise of which could result in inestimable harm to national security

Critical-Sensitive

Enzo is being vetted to be a Regional Affairs Specialist providing cultural expertise for military operations. Critical Sensitive positions like his have duties and responsibilities with the potential to cause exceptionally grave damage to national security. They automatically carry a high-risk designation. They include but are not limited to:

- Positions requiring eligibility for access to Top Secret information, as well as “Q” level information at the Department of Energy (DOE)
- Positions involving development or approval of war plans, major or special operations of war, or critical and extremely important items of war
- Positions making national security policy or determining policy
- Positions involving investigative duties, including handling counterintelligence (CI) investigations

Non-Critical Sensitive

Nora is being vetted to be a contracted software engineer working with cybersecurity systems. Non-Critical Sensitive positions like hers have duties and responsibilities that could cause significant, or serious damage to national security.

Non-Critical Sensitive positions initially carry a moderate-risk designation, unless the agency determines the position should be designated at a high level per 5 CFR Part 731 and issuances from the Office of Personnel Management (OPM). These include positions requiring eligibility for Confidential, Secret, or DOE “L” level information, and positions requiring access to automated systems that contain military active duty, guard, or reservists’ personally identifiable information.

Non-Sensitive

Clark is being vetted to be a contracted technical writer without access to classified information. Non-Sensitive positions like his are non-national-security positions that pose no potentially adverse risks to national security. These include:

- Positions that do not meet the criteria for any of the other position levels
- Positions that do not require access to classified information or performance of national security sensitive duties
- Positions of Public Trust or Suitability positions
- Positions involving physical access to DOD facilities, logical access to DOD information systems, or Homeland Security Presidential Directive (HSPD) 12 Credentialing

Special Programs

Zack is being vetted for a position as a specialist working to reduce threats to national security from nuclear materials. Special programs like these require an additional layer of security and impose access controls beyond those normally provided for Confidential, Secret, or Top Secret information.

Individuals requiring access to these programs need a more extensive national security background investigation and adjudication. These programs include:

- Presidential support activities
- Yankee White
- Special Access Programs (SAPs)
- North Atlantic Treaty Organization (NATO)
- Nuclear Personnel Reliability Program (PRP)
- Chemical PRP
- SCI
- Nuclear Command and Control Extremely Sensitive Information (NC2-ESI)

Knowledge Check 9

The new office will require a software developer who will need Secret eligibility for access to automated systems containing servicemembers' publicly identifiable information. What position designation is required for this position?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Non-Sensitive
- ○ Non-Critical Sensitive
- ○ Critical-Sensitive
- ○ Special-Sensitive

Knowledge Check 10

The new office will require an intelligence analyst with eligibility for access to Top Secret information. The position is considered to have the potential for grave but not inestimable damage to national security. What sensitivity level is required for this position?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Non-Sensitive
- ○ Non-Critical Sensitive
- ○ Critical-Sensitive
- ○ Special-Sensitive

Knowledge Check 11

The office will hire a Technical Analyst who will require access to Secret information. What tier of investigation does this fall under?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Low Tier
- ○ Moderate Tier
- ○ High Tier

Tier	Position Designation	Access
High Tier	High Risk Public Trust Critical-Sensitive Special Sensitive	Top Secret and "Q" Access Sensitive Compartmented Information
Moderate Tier	Moderate Risk Public Trust Non-Critical Sensitive	Secret/Confidential and "L" Access
Low Tier	Low Risk Public Trust Non-Sensitive	Minimum for physical/logical access and credentialing

Knowledge Check 12

The office will hire a maintenance worker who only needs a credential to enter the building. What investigative tier does this fall under?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Low Tier
- ○ Moderate Tier
- ○ High Tier

Lesson Conclusion

Lesson Summary

You have completed the *FPV Program Framework* lesson.

Lesson 5: Federal Background Investigations

Introduction

Lesson Introduction

Now that you have seen how the Federal Personnel Vetting (FPV) program is built, it's time to look more closely at the practices and processes that you and your colleagues will perform. In this lesson, we will look at the Appendices of the FPV Investigative Standards, which contain the technical and procedural information for Investigative Service Providers (ISPs) to perform their responsibilities.

Review the lesson objectives before continuing on.

- Identify the authorized Federal Investigative Service Providers
- Interpret the appendices of the FPV Investigative Standards and recognize the associated requirements

Investigative Services

Authorized Federal ISPs

The Defense Counterintelligence and Security Agency (DCSA) is the primary Investigative Service Provider (ISP) for the Federal Government. Authorized ISPs, including DCSA, conduct background investigations, including those used for national security determinations for the Department of Defense (DOD) and other Federal agencies.

When vetting for Suitability, Fitness, and Credentialing, ISPs use investigative standards, policies, and procedures defined by the Director of the Office of Personnel Management (OPM) in their role as the Suitability and Credentialing Executive Agent (Suit/Cred EA). When vetting for national security eligibility, ISPs use standards, policies, and procedures defined by the Director of National Intelligence, operating as the Security Executive Agent (SecEA).

Other investigative agencies include the Federal Bureau of Investigation (FBI) and specific areas of the Department of Homeland Security (DHS), Department of Justice (DOJ), Department of State (DOS), and Department of Transportation (DOT).

So Cole, Chris, and Suzanne, whom you met in the previous lesson, will be investigated using the standard processes you will learn about in this lesson. Completed investigations are forwarded to the authorized adjudicative facility.

Investigative Standards

Introduction to the Investigative Standards Appendices

The FPV Investigative Standards contain nine appendices. Each appendix provides detailed information on a portion of the investigative process. To learn more about this process, let’s follow Tamara Bekic as she is first hired to the DOD and then progresses through her career and the different vetting scenarios.

Tamara is being vetted for a position as a research analyst with access to Secret information. She will require a Moderate Tier investigation. You will see how ISPs obtain her personal information and ensure it is complete, relevant, and timely.

Appendix A

Appendix A, Federal Personnel Vetting Information Types and Categories, guides the collection of relevant information by providing a list of information types matched to individual attributes. The information is divided into a list of information categories that provide the precision ISPs need in their investigations:

- Citizenship and Legal Status
- Criminal History
- Education History
- Employment and Military History
- Financial History
- Foreign Activities and Associations
- Handling of Protected Information or Systems
- Identity Resolution
- Interpersonal Engagement
- Investigative and Adjudicative Records
- Non-Criminal Public Records
- Publicly Available Electronic Information
- Psychological Considerations
- Self-Provided Information
- Substance Misuse or Abuse
- Violent, Extremist, Terrorist, or Unlawful Subversive Activities

Citizenship and Legal Status

Information on Citizenship and Legal Status is used to verify an individual's U.S. citizenship or the legal status of foreign-born individuals. Using this information, we can confirm Tamara is a natural-born U.S. citizen.

Criminal History

This information is used to verify whether the individual has a criminal history from Federal, state, local, tribal, or international law enforcement. Using this information, we can see Tamara has no criminal record.

Education History

This information is used to verify an individual's education history and conduct, including attendance, dates, and degrees. Tamara's record shows she has correctly reported her completed Bachelor's and Master's degrees in Political Science.

Employment/Military History

This information is used to verify an individual's employment or military service conduct and history. Tamara attempted to join the Air Force out of high school but did not pass the medical examination. Since then, she has had a successful career as a data analyst with no evidence of deception or misconduct.

Financial History

This information is used to verify an individual's financial history, including credit reporting, liens, tax compliance, unexplained affluence, and suspicious financial activity. Tamara has good but not excellent credit and no suspicious financial activity.

Foreign Activities and Associations

This information is used to verify an individual's involvement and contact with foreign relatives and associations, businesses, or governments; foreign travel; and other foreign activities. Tamara has several relatives living in Croatia, with whom she has no contact.

Handling of Protected Information or Systems

This information is used to verify whether an individual has mishandled or misused protected information or systems, perhaps through unauthorized disclosures or misused resources. There is no indication Tamara has ever compromised the proprietary information she has handled in her career. She has never had access to classified information.

Identity Resolution

This information is used to verify that the individual is who they purport to be. Tamara's identity is resolved successfully.

Interpersonal Engagement

This information is gathered by contacting personal sources to gain insight and context about the individual's personal interactions. The goal is to reveal attributes relevant to trust determinations. Tamara's personal sources, including

former teachers, colleagues, and relationship partners, describe her as calm, intelligent, and respectful.

Investigative and Adjudicative Records

This information is used to verify an individual's current and prior background investigation, continuous vetting, adjudication, and clearance history. Tamara has no investigative and adjudicative history predating this investigation.

Non-Criminal Public Records

This information is used to verify any non-criminal public records that may be relevant to a trust determination, such as lawsuits, name changes, or divorce records. These records show no adverse information for Tamara.

Publicly Available Electronic Information

This information is gleaned from an individual's associations, behaviors, or conduct from their publicly available online presence and activities, including social media, the deep web, or the dark web. Tamara has very little social media presence outside discussions of mystery novels.

Psychological Considerations

This information is used to verify if an individual has mental health psychological conditions that are relevant to trust determinations, evidence of treatment, and evidence of progress or outcomes. Tamara's records show she experienced a major depression several years ago after a medical event, and no other conditions since.

Self-Provided Information

This information is used to verify an individual's claims through resumes, questionnaires, and other forms of self-reporting that may identify or clarify indicators of potential concern in other categories. Tamara's records show no concerning issues.

Substance Misuse or Abuse

This information is used to verify if an individual has misused or abused substances and evidence of rehabilitation. Tamara has no record of substance misuse or abuse.

Violent, Extremist, Terrorist, and Unlawful Subversive Activities

This includes information about an individual's actions against the Government or involvement with others in plans or actions against the government. Tamara has no record of violent, extremist, or subversive activities.

Appendix B

(CUI) Since this is Tamara's first Federal position, she will receive her Initial Vetting. Appendix B, Initial Vetting Coverage Requirements, provides tables describing the data sources and methods to be used for each information category, for each investigative tier. DCSA and any other authorized ISPs are required to conduct the Initial Vetting in accordance with these requirements.

(CUI) Since Tamara has applied for a Moderate Tier position, coverage requirements include tasks like checks of credit bureau reporting agencies to verify her financial status, checks of law enforcement records and court records for her legal history, and a check of DHS records on personal foreign travel and other foreign connections.

Appendix C

(CUI) Once Tamara receives a favorable trust determination, she will be enrolled in Continuous Vetting (CV). Appendix C, Continuous Vetting Coverage Requirements, provides tables describing the minimum standards and time periods for each investigative tier, including whether the check is made periodically or by subscribing to automated alerts.

(CUI) The CV program must meet the required time- and event-driven checks at the appropriate tier based on the position. For Tamara, that means CV at the Moderate Tier. The CV program must also integrate agency-specific information at all levels into the CV process. The program must use alert management processes to evaluate and address issue information that may arise on Tamara's record as it emerges. By administrating the CV program under these requirements, the program can help to maintain the Government's confidence that trusted insiders like Tamara will continue to protect People, Property, Information, and Mission, and support her mobility within the trusted workforce.

(CUI) For Tamara's Moderate Tier position, examples of CV data sources include daily checks of the appropriate terrorist databases, annual credit bureau checks for financial information, and automated alerts from the FBI Records Management Division to check for Tamara's name in new investigation files.

Appendix D

(CUI) Let's fast forward a few years. Tamara has done well in her position and will now be assigned Top Secret projects, meaning her position now has High Tier requirements and Tamara's vetting requires an Upgrade. Appendix D, Upgrades Coverage Requirements, describes the investigative standards for insiders like Tamara whose positions are re-designated at a higher tier. It also describes requirements for those moving to a new position requiring a higher-tier investigation within their agency, and it may also apply to certain insiders moving to a higher-tier position in another agency.

(CUI) Since Tamara has already received her Initial Vetting and been continuously enrolled in CV, she only needs the vetting that will meet the investigative requirements for the new tier. For Tamara, her redesignation to the High Tier would include FBI criminal record checks for her spouse as well as herself, a check for any new education records not previously obtained, and an individual interview to develop a full understanding of her personal history.

Appendix E

One year after her upgrade, Tamara transfers to a High Tier position in another DOD agency. This will require a Transfer of Trust. Appendix E, Transfer of Trust Coverage Requirements, describes how the ISP supports agencies to enhance the mobility of trusted insiders like Tamara.

Her new agency must review the level of investigation that has been conducted, her CV enrollment status, and her previous adjudicative determination record. Based on the review, the agency may request the ISP to conduct additional vetting, but they must only request the vetting necessary to meet the needs of the new position and address any new information. For example, if Tamara's new position required access to Sensitive Compartmented Information or Special Access Programs, her new agency could request additional checks beyond the requirements for a High Tier position. Given that her new position does not have these requirements, however, the new agency must reciprocally accept Tamara's previous determination.

Appendix F

Now suppose Tamara, like many insiders, leaves the Federal workforce for a time and then seeks to return. At that point she will need to re-establish trust. Appendix F, Re-establishment of Trust Coverage Requirements, describes how the ISP can support agencies when former trusted insiders seek to return to work for or on behalf of the Federal Government.

Agencies have different requirements depending on the length of the *break in service*, the time period when an individual is no longer in a position that requires personnel vetting. If Tamara's break in service lasts less than 36 months, her new agency will need to apply the instructions from the Vetting Scenario Implementation Guidance to determine whether to accept the previous background investigation, CV activities, and trust determination.

If her break in service is between 36 months and five years, her agency will request the ISP conduct any Initial Vetting necessary to cover the duration of the break in service, meet the needs of the position, and address any new information.

If the break in service is more than five years, she will require a new Initial Vetting.

Provided Tamara receives a favorable trust determination, her new agency must then reenroll Tamara in Continuous Vetting.

Appendix G

Now, consider what would happen if Tamara's background investigation revealed issues requiring evaluation by an adjudicator. Appendix G, Issue and Case Seriousness Categorization, contains the categories ISPs utilize to identify the seriousness of individual issues and overall cases, as well as reporting protocols.

Cases are categorized based on the seriousness of the issues, from a categorization of:

- No Issues, indicating the case contains no issues or inconsistent information
- Minor, indicating the case contains conduct or issues that are minor in nature
- Moderate, indicating conduct or issues could be of moderate concern when making a determination
- Substantial, indicating conduct or issues likely of substantial concern when making a determination
- Major, indicating conduct or issues that could be of major concern

If a standalone issue is uncovered during the investigation that prompts a Substantial or Major case seriousness category, the ISP must alert the requested agency. ISPs will then continue the investigation unless the agency directs otherwise.

If the ISP gains firsthand knowledge of information that an individual could pose an imminent threat to the safety or security of themselves, another individual, or a facility, it is imperative the ISP use good judgment in determining that the threat is

credible and critical, before taking appropriate action to immediately notify the proper law enforcement agency, Federal agency, or military command.

Appendix H

(CUI) Throughout Tamara's career, she has been vetted in all five scenarios. Appendix H, Federal Personnel Vetting Investigative Methodologies, established the spectrum of investigative methodologies that ISPs used to collect her information. ISPs have flexibility within these parameters to select the most efficient and cost-effective methodology, so long as it can obtain the information identified in the Standards and Appendices.

(CUI) Investigative methodologies are divided into three bands. Band 1 includes methods expected to require a minimal level of effort and often does not involve manual processing or human intervention. Band 2 includes methods expected to require an increased level of effort and may involve remotely conducted record requests and reviews, interviews with personal sources, or interviews with the individual. Band 3 includes methods expected to require the highest level of effort, including in-person contact or video teleconferencing with record providers, sources, or the individual.

(CUI) Now think back to Tamara's Upgrade vetting, when she moved from a Moderate Tier position to a High Tier position. That investigation required ISPs to collect information about her spouse's criminal history and her recent education history, as well as to conduct an individual interview. An automated check of Federal investigation records would fall under Band 1, telephone or electronic contacts with educational institutions would fall under Band 2, and her individual interview would fall under Band 3.

Appendix I

(CUI) If, at any point during Tamara's vetting, potentially adverse information comes to light that requires evaluation, Appendix I, Investigative Triggers and Required Actions, provides the specific criteria or thresholds of information that will result in an investigative trigger and the required actions for each tier. Any issues that have previously been investigated or adjudicated to the applicable standards do not qualify as a current trigger, unless there is new information, a pattern of behavior is identified, or the issue extends into the current investigation.

(CUI) In the event of a trigger, the ISP must address and report all pertinent facts and circumstances necessary to fully address the issues and any other perceived vulnerabilities that may arise during the expansion of the investigation. The ISP must also ensure that the investigation contains the coverage required for the individual's

vetting scenario, unless otherwise specified. Finally, the ISP must ensure all issues have been fully addressed and reported per the requirements of Appendix I.

(CUI) Consider again Tamara's Upgrade to a High Tier position. If one of the listed educational institutions had contradicted Tamara's self-reported information, Appendix I would have required the ISP to conduct a triggered interview to give Tamara an opportunity to address the discrepancy.

Knowledge Check 1

Which of these organizations is the primary ISP for the Federal Government, conducting background investigations, to include those used for national security determinations for DOD and other Federal agencies?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Office of Personnel Management (OPM)
- ○ Department of Transportation (DOT)
- ○ Department of Justice (DOJ)
- ○ Defense Counterintelligence and Security Agency (DCSA)

Knowledge Check 2

A DCSA investigator uncovers a detail in an individual's work history that prompts the overall case seriousness to Major. The investigator completes the investigation and documents an alert for the adjudicator. Which Appendix provides this guidance?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Appendix A: FPV Information Types and Categories
- ○ Appendix E: Transfer of Trust Coverage Requirements
- ○ Appendix G: Issue and Case Seriousness Categorization
- ○ Appendix I: Investigative Triggers Required Actions

Knowledge Check 3

(CUI) Samantha currently holds a Moderate Tier position in the DOD. An annual check of her credit status reveals troubling financial concerns. Which Appendix describes this process?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Appendix A: FPV Information Types and Categories
- ○ Appendix C: Continuous Vetting Coverage Requirements
- ○ Appendix D: Upgrades Coverage Requirements
- ○ Appendix H: FPV Investigative Methodologies

Knowledge Check 4

ISPs must ensure that background investigations cover all 16 types of information needed to make a determination of whether an individual can be a trusted insider. Which Appendix provides this guidance?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Appendix A: FPV Information Types and Categories
- ○ Appendix B: Initial Vetting Coverage Requirements
- ○ Appendix G: Issue and Case Seriousness Categorization
- ○ Appendix H: FPV Investigative Methodologies

Knowledge Check 5

Matthew is a Federal employee with access to Top Secret information. He has accepted a position as a contractor with the same level of access. Which Appendix describes this vetting scenario?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Appendix B: Initial Vetting Coverage Requirements
- ○ Appendix D: Upgrades Coverage Requirements
- ○ Appendix E: Transfer of Trust Coverage Requirements
- ○ Appendix F: Re-establishment of Trust Coverage Requirements

Lesson Conclusion

Lesson Summary

You have completed the *Federal Background Investigations* lesson.

Lesson 6: Federal Adjudications

Introduction

Lesson Introduction

When the background investigation is complete, Federal adjudicators must weigh the candidate's whole character and history to determine whether that person represents a risk to the Federal service and to national security.

In this lesson, you will learn about the principles and procedures adjudicators use to make trust determinations. Review the lesson objectives before moving on.

- Summarize the Common Principles in Applying Federal Personnel Vetting Adjudicative Standards.
- Explain the Whole Person Concept.
- Describe personnel vetting standards for rendering a trust determination for eligibility to access classified information or to hold a sensitive position.
- Apply requirements for making preliminary determinations and temporary eligibility determinations for access to classified information.

Adjudicative Policy

The Common Principles

The Common Principles in Applying Federal Personnel Vetting Adjudicative Standards contains the policy requirements for the adjudicative process. It describes the adjudicative principles that are common to all Executive Branch-authorized adjudicative entities and underscores the characteristics that are expected from the entire trusted workforce: good conduct, integrity, sound judgment, loyalty, and reliability.

The Common Principles also outline an adjudicative process framework to promote consistency and fairness in the adjudicative process across all personnel vetting domains—initial vetting, continuous vetting, upgrades, transfers of trust, and re-

establishment of trust—for any individual, including Federal civilians, military personnel, and contractors, except as provided by law, regulation, or policy.

Agency and Adjudicator Responsibilities

Adjudicative trust determinations are inherently governmental responsibilities, not to be performed by anyone outside the Federal workforce, and federal agencies must ensure that adjudications are performed to the strict standards set down by law and policy. Agencies must ensure adjudicator training meets educational requirements, including training in unconscious bias and ethnic and cultural differences. Agencies must use Executive Agent-approved automated capabilities to the greatest extent practicable. They must reciprocally accept trust determinations made by other agencies. Finally, federal agencies must ensure that adjudicators comply with all essential requirements.

Adjudicators must:

- Use relevant, timely, and complete information when making adjudications
- Use the adjudicative process framework and vetting criteria
- Treat all individuals with fairness, dignity, and respect
- Recuse themselves from conflicts of interest
- Properly protect, use, share, transmit, and retain information
- Refer adjudicatively relevant information to law enforcement, counterintelligence, insider threat, or other authorities as necessary
- Comply with quality oversight measures

Adjudicative Process Framework

Adjudicators use the Adjudicative Process Framework laid down by the Common Principles to evaluate the information they receive and make a trust determination. The Framework is broken into four key components: the investigation, the order of operations, the process of risk assessment, and preliminary determinations. This adjudicative process framework culminates in a trust determination for each applicable personnel vetting domain.

First, determinations are informed by Investigations, which provide complete and relevant data and contextual information related to the individual’s behaviors and perceived vulnerabilities, allowing for a balanced and comprehensive assessment of both positive and negative information, to the extent applicable.

The adjudicator will apply this information to each of the applicable domains for the candidate, following a specific Order of Operations. The adjudicator starts with Suitability or Fitness, then National Security Eligibility, and then Credentialing.

After applying the adjudicative criteria for the domain, the adjudicator carries out a Risk Assessment. If there are no issues or the issues can be mitigated, the adjudicator makes a favorable trust determination. If issues are present, the adjudicator will conduct further analysis.

Investigation

Taran is being vetted for a High Tier position in the Intelligence Community (IC). The adjudicator can only make a trust determination about Taran if they have sufficient information about his character and history.

Investigative Service Providers (ISPs) must collect a sufficient amount of information for adjudicators to make a determination, though adjudicators may also receive information about Taran from individual or non-ISP entities. If a determination cannot be made based on the information available, an adjudicator may return the case to the ISP for further investigation.

Order of Operations

Trust determinations are made in a strict sequence, depending on which of the four domains apply to the individual's case. First, Taran will be vetted for his Suitability or Fitness for the position. Then, he will be vetted for National Security Eligibility to access Top Secret information.

If he is adjudicated favorably for the other domains, Taran is eligible for a credential without a separate adjudication, though the credentialing trust determination and issuance must still be recorded in his Federal personnel vetting record.

It is possible for Taran to receive a favorable trust determination for one domain, but an unfavorable trust determination for another.

Risk Assessment

The goal of the adjudicative process is to determine whether insiders or potential insiders like Taran present a risk to People, Property, Information, and Mission. Will Taran be a risk to the Federal service or national security? Can the risk be mitigated?

This focus on Risk Assessment makes it all the more important for adjudicators to validate that the information from Taran's investigation meets the Quality

Assessment Standards. If issues arise that require additional information to resolve, the adjudicator should request further investigation.

Preliminary Trust Determinations

Taran has applied for a specialized position, and the agency has an urgent need for someone to support their mission. The head of the agency, or their authorized security personnel, may approve a preliminary trust determination while the adjudication process is still being completed. These decisions are made on a case-by-case basis. We will discuss these in more detail later in this lesson.

Whole Person Concept

To demonstrate that Taran is not a risk to national security, adjudicators must adhere to the Whole Person Concept, examining a sufficient period of Taran's life and carefully weighing a number of variables to determine whether he is an acceptable security risk. All available, reliable information about the individual, past and present, favorable, and unfavorable, must be considered in reaching a national security eligibility determination.

All cases are unique, and the adjudicator must make a determination based on Taran's individual merits.

Knowledge Check 1

Which of the following are defined in the Common Principles in Applying Federal Personnel Vetting Adjudicative Standards?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ The Order of Operations for trust determinations
- ☐ HSPD-12 Credentialing standards
- ☐ Federal Personnel Vetting Guidelines
- ☐ Guidelines for preliminary trust determinations

Knowledge Check 2

Which of the following are defined in the Common Principles in Applying Federal Personnel Vetting Adjudicative Standards?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ Position designation categories

- ☐ Appeal processes for legal whistleblowers
- ☐ Guidance for risk assessment
- ☐ Adjudicative Process Framework

Knowledge Check 3

Liqiao is a naturalized U.S. citizen being vetted for national security eligibility. Which of the following statements is true about the adjudication process for Liqiao?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ The adjudication will not consider events that took place before Liqiao immigrated to the United States from China.
- ○ All available, reliable evidence about Liqiao should be considered to make a determination, no differently from other cases.
- ○ Adjudicators will use guidelines specialized for Chinese-American citizens to evaluate Liqiao's case.
- ○ Liqiao's political and cultural activities must be given greater weight than those of native-born citizens.

Trust Determinations

Introducing Trust Determinations

Now that you've learned the policy for adjudications, it's time to review the adjudicative process.

Consider these new employees, both of whom will need access to classified information. Toby is being vetted for a program management position. It has been seven years since he was last in the Federal workforce, so to re-establish trust, Toby is undergoing new Initial Vetting for Suitability, National Security, and Credentialing.

Miles is being vetted for a position as a contracted data analyst. This will be his first time in the Federal workforce, so he is also undergoing Initial Vetting for Fitness, National Security Eligibility, and Credentialing.

The ISP will provide the authorized adjudicative facility with completed background investigations for these two individuals to serve as the basis for the adjudicative decisions. Investigators should be familiar with the types of adjudications to understand the kinds of information adjudicators are required to consider, and to ensure their investigative products meet the needs of the adjudicator.

Suitability and Fitness

Toby's first determination will be for his suitability for the new position. Suitability refers to identifiable character traits and conduct that indicate the individual is likely to be able to carry out the duties of a Federal job with integrity, efficiency, and effectiveness. It is evaluated using facts from 5 Code of Federal Regulations (CFR) Part 731.

Because Miles is being vetted for a contractor position, he will instead be vetted for Fitness. Fitness is the level of character and conduct determined necessary for an individual to work for or on behalf of a Federal agency in a position not subject to suitability.

The Office of Personnel Management (OPM) establishes minimum adjudicative criteria for fitness determinations, though the heads of agencies retain the discretion to establish additional adjudicative criteria.

Evaluating Suitability

Toby's Suitability adjudication process will be broken into two steps using factors found in 5 CFR Part 731. First, the adjudicator performs a basic evaluation of the individual's Suitability for entry into Federal employment. If a basic evaluation reveals no issues, the adjudicator may proceed with a full, job-specific evaluation, and determine:

- Whether Toby demonstrated misconduct or negligence in employment
- Whether Toby demonstrated criminal or dishonest conduct
- Whether he provided material, intentional false statement, or deception or fraud in examination or appointment
- Whether he refused to furnish testimony
- Whether he has a history of alcohol abuse, without evidence or substantial rehabilitation, of a nature and duration suggesting he could not perform the duties of the position or would be a direct threat to others
- Whether he has a history of illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation
- Whether he knowingly and willfully engaged in acts or activities designed to overthrow the U.S. Government by force
- Whether there is any statutory or regulatory bar preventing his lawful employment in the position

Case File: Toby Marlow

Toby's record shows that, four years ago, while he was out of the Federal workforce, he was dismissed from a position for working while intoxicated with alcohol. After learning this, OPM and the hiring agency should then review the additional considerations and determine whether any are pertinent.

- What is the nature of the position Toby has applied to?
- What is the nature and seriousness of the conduct?
- What are the circumstances surrounding the conduct?
- How recent was the conduct?
- How old was the individual at the time?
- Did any societal conditions contribute to the conduct?
- Is there any evidence of rehabilitation or efforts toward rehabilitation?

Now consider Toby. He has applied for a management position with access to Top Secret information. An employee abusing alcohol in this position could cause damage to the service and the public trust. By Toby's own self-report, his actions while abusing alcohol caused financial consequences for his company. He has admitted that he went through a period of depression following the death of a close family member, and although the conduct was within the last five years, Toby received counseling for his alcohol abuse and states he has been continuously sober for three years.

The adjudicator in this case must review the conduct and the circumstances, together with Toby's other traits and characteristics, to determine whether he will pose a risk in the new position.

National Security Eligibility

Once Miles and Toby have received favorable trust determinations for their Suitability or Fitness for the position, they will be evaluated for eligibility to access national security information. The national security adjudication seeks reasonable assurance that Miles is loyal, trustworthy, and reliable to the degree required for access to classified information. The adjudicator will consider his stability, discretion, character, honesty, and judgment, doing so in a way that is consistent and fair, evaluating both past and present, and favorable and unfavorable information.

Evaluating Eligibility

The adjudicator on Miles's case will use the 13 National Security Adjudicative Guidelines found in Security Executive Agent Directive (SEAD) 4. These guidelines describe

- His allegiance—including his allegiance to the United States and any foreign influence or foreign preference
- His character—including sexual behavior, personal conduct, and financial considerations
- His health—including alcohol consumption, drug involvement and substance misuse, and psychological conditions
- His behavior—including criminal conduct, handling protected information, outside activities, and use of information technology

Each guideline has three components. The *concern* explains why the behavior might pose an unacceptable risk to national security. The *disqualifying conditions* indicate specific conduct and behavior that could raise a security concern. The *mitigating conditions* may lessen the severity of the security concern and could permit a favorable determination. Continue on to examine Miles's record.

Factors to Evaluate

Three years ago, Miles was disciplined by an employer for making changes to a live information system without approval. This behavior falls under Adjudicative Guideline M: Use of Information Technology. The concern is that failure to comply with rules for using information technology systems could call into question Miles's ability to protect classified information. The disqualifying condition is the action itself, the unauthorized modification of an information technology system.

When evaluating the disqualifying condition, the adjudicator has several factors to consider:

- The nature, extent, and seriousness of the conduct
- The circumstances surrounding the conduct, including the individual's knowledgeable participation
- The frequency and recency of the conduct
- The individual's age and maturity at the time of the conduct
- The extent to which their participation was voluntary

- The presence or absence of rehabilitation and other permanent behavioral changes
- The motivation for the conduct
- The potential for pressure, coercion, exploitation, or duress because of the information
- The likelihood of continuation or recurrence

Using these factors, the adjudicator can better characterize the risk that this issue may create for national security.

Mitigating Conditions

As with Suitability and Fitness, in evaluating the relevance of the issue, the adjudicator will consider any mitigating conditions around Miles's conduct. The adjudicator should consider how much time has elapsed since the behavior and the circumstances in which it happened. This can help the adjudicator determine whether the incident is likely to recur and demonstrate Miles's reliability, trustworthiness, or good judgment.

The adjudicator should also consider whether the misuse of the system was minor, and whether it was done solely in the interest of organizational efficiency and effectiveness; whether the misuse was unintentional or inadvertent, and whether Miles tried to correct the situation and notified appropriate personnel; and whether the misuse was due to improper or inadequate training or unclear instructions.

Now what about Miles? The incident happened fairly recently, within the last five years, and according to Miles's employment records, it required several weeks of work to rebuild company databases. While Miles did notify his employer and took good-faith effort to correct the incident, the employer states the incident was caused by Miles's negligence. Using this information, the adjudicator can make a better judgment about any risk that Miles may pose in the position.

Additional Factors for Trusted Insiders

If Miles already has access to classified information when the incident comes to light, SEAD 4 provides a different set of questions for adjudicators to consider.

- Did Miles voluntarily report the incident?
- Was he truthful and complete in responding to questions about incident details?

- Did he seek assistance and follow professional guidance during or after the incident?
- Does he appear likely to favorably resolve this concern?
- Has he demonstrated positive changes in behavior?

The adjudicator also needs to ask whether Miles poses enough risk that his current eligibility should be suspended pending final adjudication of the issue.

Exceptions

If the adjudicator determines Miles's previous behavior poses a risk to national security, they could make an unfavorable determination in his case. The hiring agency could also make an exception. An exception is an adjudicative decision to grant initial or continued eligibility for access to classified information or hold a sensitive position *despite* an individual's failure to meet the full adjudicative or investigative standards.

A Waiver indicates eligibility can be granted or continued despite the presence of substantial issue information that would normally preclude eligibility. A waiver may only be approved when the benefit of eligibility clearly outweighs any security concerns.

A Condition indicates eligibility may be granted or continued despite the presence of issues that can be partially but not completely mitigated, provided additional security measures are required to mitigate the issue, including security monitoring, access restrictions, periodic financial statements, or attendance at counseling sessions.

A Deviation indicates eligibility may be granted or continued despite a significant gap in coverage or scope of the investigation. A significant gap would mean either a complete lack of coverage for a period of six months or longer within the most recent five years investigated, or the lack of one or more relevant investigative scope components in its entirety.

An Out of Scope exception indicates reinvestigation is overdue.

Credentialing

Let's check in on Toby. If he receives favorable trust determinations for Suitability and National Security Eligibility, he receives a Credentialing determination. The standards for credentialing within the DOD are found in Department of Defense Instruction (DODI) 5200.46.

In general, a favorable trust determination will be made unless there is substantiated disqualifying information that cannot be mitigated. A Common Access Card (CAC) will not be issued to Toby:

- If he is known to be or reasonably suspected of being a terrorist
- If the employer is unable to verify his claimed identity
- If there is a reasonable basis to believe Toby has submitted fraudulent information about his identity
- If there is a reasonable basis to believe he will attempt to gain unauthorized access to classified or protected information
- If there is a reasonable basis to believe he will use the credential outside the workplace unlawfully or inappropriately
- If there is a reasonable basis to believe he will use controlled information systems unlawfully, make unauthorized modifications to them, or otherwise corrupt, destroy, or misuse them

If Toby's determination is favorable, his CAC may be approved and issued on an interim or final basis. If the interim determination is unfavorable, then issuance of the CAC will be deferred pending receipt and adjudication of the investigation report. An unfavorable trust determination at this stage means a CAC may not be issued.

Credentialing Without Other Vetting

In some situations, hiring agencies may need to vet someone for a credential who does not require vetting for suitability or fitness, or for national security eligibility, such as Amelie. In her case, the agency has the flexibility to apply supplemental standards to ensure that granting the credential does not create unacceptable risk. These standards could include:

- Misconduct or negligence in employment
- Criminal or dishonest conduct
- Material, intentional false statements, deception, or fraud
- Alcohol abuse without evidence of substantial rehabilitation
- Illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation
- The existence of any statutory or regulatory bar that would prevent the individual's employment

- Knowing and willful actions designed to overthrow the U.S. Government by force

Knowledge Check 4

Noelle Kirkpatrick is being vetted for a position handling Secret Information. During her Initial Vetting for National Security Eligibility, the adjudicator finds that four years ago, she was terminated from a position while managing an opioid use disorder. Which of the following must the adjudicator consider as they review her record?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ Whether the substance misuse occurred after a severe or prolonged illness or injury
- ☐ How many other candidates for the position have shown the same conduct
- ☐ The presence or absence of rehabilitation and other permanent behavior changes
- ☐ Not applicable; the adjudicator must make an unfavorable determination when opioid misuse is involved.

Knowledge Check 5

Joseph Kim is being vetted for Suitability for a High-Risk position. Which of the following factors must be considered from 5 CFR Part 731?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ Material, intentional false statement
- ☐ Misconduct or negligence in employment
- ☐ Political or religious affiliation
- ☐ Educational attainment

Knowledge Check 6

Leonard Navarro is currently a trusted insider with access to Top Secret information. As part of his Continuous Vetting, the adjudicator is evaluating Leonard’s current

difficulties meeting financial obligations. Which of the following must the adjudicator consider?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ Whether Leonard performs volunteer or charity work in the community
- ☐ Whether Leonard has self-reported the information.
- ☐ Whether Leonard has sought professional financial assistance to resolve his debt
- ☐ Whether Leonard is demonstrating positive changes in financial behavior

Knowledge Check 7

Chelsea Shaw is being vetted for her Suitability for a Moderate-Risk position. Which of the following issues indicate factors that must be considered from 5 CFR Part 731?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ Chelsea did not report that she was terminated from a previous position for cause.
- ☐ Chelsea was a member of a sorority in college.
- ☐ Ten years ago, Chelsea had a restraining order placed against her by an ex-partner.
- ☐ Chelsea does not drink alcohol.

Knowledge Check 8

Catalina Morales is being vetted for Credentialing for access to a Federal worksite. Which of the following information could disqualify Catalina from receiving a credential?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ There is a reasonable basis to believe Catalina will use a credential outside the workplace inappropriately.
- ☐ Catalina has never been charged with a crime.
- ☐ Catalina does not meet the agency's supplementary credentialing standards.
- ☐ Catalina was injured in an auto accident seven months ago.

Preliminary and Temporary Determinations

Preliminary Determinations

In a previous lesson, you met Gabriel. He is being vetted for an Upgrade as he is being promoted to a supervisor position. There is important work to be done in the position, and the head of the agency would like Gabriel to start right away. In this case, the agency head, or security personnel they authorize, could make a preliminary determination to allow Gabriel to begin before the adjudication has concluded.

Preliminary determinations are internal decisions based on findings from high-yield checks. If the agency has an urgent need and is confident Gabriel will receive a favorable trust determination, they can get him to work quickly prior to completing the investigative coverage requirements.

Temporary Access to Classified Information

Agency heads, or security personnel they designate, also have the authority to make temporary or one-time eligibility determinations, either for individuals who do not have access to classified information or for those who have access to a lower level, when determined necessary to meet operational or contractual needs that are not expected to recur, as required by Executive Order 12968. The requirements for temporary access are outlined in SEAD 8.

For temporary access to Confidential, Secret, or L information, the individual must have received: a favorable review of a completed Standard Form (SF) 86, the Questionnaire for National Security Positions; a verification of their citizenship; initiation of an expedited investigation, and completion and favorable review of an FBI fingerprint check.

For access to Top Secret and Q information, the individual must have a favorable review of their completed SF 86, citizenship verification, initiation of an expedited investigation, and favorable reviews of an FBI Fingerprint Check, an FBI name check, and a National Crime Information Center (NCIC) check.

Knowledge Check 9

Ruth is a DOD Paralegal Specialist with eligibility and access to Secret information. She will require temporary access to Top Secret information while working a court

case that is expected to last nine months. Which of the following must be accomplished for her to obtain access?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ Favorable review of SF 86
- ☐ Citizenship verification
- ☐ Favorable review of FBI and NCIC law enforcement checks
- ☐ Initiation of an expedited investigation

Knowledge Check 10

Jude is receiving his Initial Vetting for a Federal position, and the agency head is considering authorizing a preliminary trust determination. Which of the following are true?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ The preliminary determination must be based on information from high-yield checks.
- ☐ Jude must receive a favorable Credentialing determination before preliminary access can be authorized.
- ☐ The agency must receive Executive Agent permission to authorize a preliminary determination.
- ☐ The agency head may authorize security personnel to make the determination.

Lesson Conclusion

Lesson Summary

You have completed the *Federal Adjudications* lesson.

Lesson 7: Federal Personnel Vetting Record

Introduction

Lesson Introduction

The Federal Personnel Vetting (FPV) program is essential to the protection of People, Property, Information, and Mission. The information that is collected, used,

and stored for investigations and trust determinations must also be protected. In this lesson, you will learn about the practices for recording and safeguarding FPV information.

Review the lesson objectives before moving on.

- Describe how trust determinations are recorded and reported in internal security systems that feed government-wide repositories.
- Apply guidance on appropriate protection and handling of investigative case file materials.
- Given a scenario, apply the requirements for the safeguarding, handling, and retention of personnel vetting records.

Safeguarding FPV Records

Recording FPV Information

During the vetting process, adjudicators must record personnel vetting actions and trust determinations in an individual's Federal Personnel Vetting (FPV) record. Accurately recording FPV actions and determinations promotes transparency, enhances mobility, and facilitates information sharing.

The adjudicative entity is responsible for recording personnel vetting actions and trust determinations in an individual's FPV record, unless they are authorized to withhold information pursuant to law, regulation, or policy. The head of the adjudicative entity may authorize an agency to withhold information about certain individuals from the database if they consider it necessary for national security purposes.

The FPV record includes:

- Preliminary determinations, including temporary eligibility and access
- Trust determinations, and reciprocal acceptance of trust determinations, for all FPV scenarios and domains
- Classified information eligibility levels and the date eligibility was granted
- The adjudication of new Continuous Vetting and developed information
- Any exceptions granted

- The status of special cases like suspensions, revocations, separations, open or unadjudicated investigations, loss of jurisdiction, and proceedings for due process, appeal, or redress
- Issuance of a credential, or denial, suspension, or revocation of credentialing eligibility
- The dates of polygraphs and the administering agency

Protecting FPV Information

Recall Naomi from a previous lesson. She is being vetted for a position that will require a High Tier investigation. During and after her vetting, background investigators and adjudicators are responsible for adequately protecting her FPV records.

Good information management and safeguarding practices are essential to good government, maintaining the trust of the public and the workforce, and the quality and effectiveness of operations. While Executive Order 13467, Section 1.1 (e), allows agencies to release records in certain situations, any redisclosure should be coordinated with the Freedom of Information Act (FOIA) Office for Investigations to ensure that the redisclosure does not violate statutory restrictions or result in unauthorized disclosure.

Let's review how this works in practice.

Case File: Naomi Nuñez

Naomi is undergoing High Tier vetting for a position that could cause inestimable damage to national security in the wrong hands. How can the agency recognize whether her case information is being properly handled and protected?

Information collection and management practices must promote the Government's ability to attract talented and trustworthy individuals, like Naomi hopefully is. An unfair or unsecured vetting process could drive away the people the Government needs to recruit.

The information used to make Naomi's trust determination, and to manage her risk to national security, should be accurate, relevant, timely, and as complete as reasonably necessary, to ensure she is treated fairly. Remember, she must be evaluated through the Whole Person Concept.

Information collection should not be unduly intrusive. It should be appropriately tailored to the requirements for Naomi's case.

Vetting practitioners should be engaged with Naomi during the entire vetting process to collect information, resolve derogatory information, improve transparency, and cultivate effective two-way communication between her and the Government.

The agency's staff should be trained and vetted to be accountable for the protection of information, including information shared by complementary missions, and mechanisms should be in place to safeguard FPV sources and methods, and to protect the collection, use, dissemination, and retention of information.

The agency should maximize efficiencies in managing information through cooperation and timely sharing of relevant information among complementary missions, both between and within agencies.

The agency should use a risk-based approach to identify and detect potential vulnerabilities and threats early in the process, and to undertake risk mitigation throughout the process to lessen or prevent the impact to People, Property, Information, and Mission.

These are the practices that define the proper management and safeguarding of information.

Knowledge Check 1

Benjamin is undergoing Initial Vetting for Top Secret eligibility and access. Which of the following actions correctly apply the requirements to safeguard personnel vetting information?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ The background investigator reviews the gathered information to verify that it is relevant and timely.
- ☐ The adjudicator making the determination is properly trained in information security.
- ☐ The adjudicator deletes information from Benjamin's file that they do not believe is relevant.
- ☐ The background investigator provides Benjamin with several records from his personnel vetting file.

Knowledge Check 2

Annie is transferring to a new Federal position with the same level of risk and access as her current position. Which of the following information must be documented in her FPV record?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ The reciprocal acceptance of Annie's previous trust determinations
- ☐ Any exceptions that may apply to Annie's national security eligibility
- ☐ The date Annie's polygraph examination takes place
- ☐ Any information that is withheld from the database for national security purposes

Knowledge Check 3

Connie is being vetted for an Upgrade to Top Secret eligibility and access. Which of the following actions correctly apply the requirements to safeguard personnel vetting information?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ The adjudicator discusses information collection methods over unsecured media.
- ☐ The information collection process is not unduly intrusive.
- ☐ The adjudicator uses a risk-based approach to identify vulnerabilities and threats.
- ☐ Information sharing between agencies makes the process more efficient.

Lesson Conclusion

Lesson Summary

You have completed the *Federal Personnel Vetting Record* lesson.

Lesson 8: Course Conclusion

Course Summary

Summary

In this course, you learned about the foundational laws, policies, and other guidance upon which the Federal Personnel Vetting program is built. You learned how the program is conducted by background investigators and adjudicators, including key processes and guidelines.

Exam Instructions

Congratulations! You have completed the *Overview of Federal Personnel Vetting* course. You should now be able to perform the listed activities.

- Given a description, determine the governing documents and principles related to the Federal PV program and the judicial cases and practices that have influenced the personnel vetting process.
- Given a description, determine the Federal Personnel Vetting Policy Framework and procedures for making trust determinations.

To receive course credit, you must take the *Overview of Federal Personnel Vetting* exam. If you accessed the course through the Security Training, Education, and Professionalization Portal (STEPP), please use that system to access the online exam.

Appendix A: Answer Key

Lesson 2 Review Activities

Knowledge Check 1

Frances, a Federal employee with access to Secret-level information, recently filed a lawful whistleblower complaint relating to work performed in her office. Now she is being vetted for access to Top Secret information. How does 50 USC § 3234 impact her case?

- ⦿ Frances's trust determination may not be denied on the basis of her complaint. (correct answer)
- ○ Information about Frances's whistleblower action is exempted from FOIA requests.
- ○ Lawful whistleblowers must not have access to Top Secret information.
- ○ Frances must be granted Top Secret clearance by default.

***Feedback**: 50 USC § 3234 specifies that Frances's trust determination may not be denied on the basis of her whistleblower action.*

Knowledge Check 2

Walter is being vetted for a role accessing Secret information. How does the Privacy Act of 1974 impact his case?

- ○ Walter has waived all privacy rights during the vetting process.
- ⦿ It allows Walter to access his own personnel records, unless information is exempted for national security reasons. (correct answer)
- ○ Walter is prohibited from becoming a whistleblower.
- ○ Walter's information may not be stored in a secure database.

***Feedback**: According to the Privacy Act of 1974 Walter generally must be notified and give consent for his information to be used.*

Knowledge Check 3

Miranda is an information security specialist transferring to a new agency within the DOD. How does Executive Order 13488 apply to her case?

- ⦿ E.O. 13488 requires Miranda's new agency to reciprocally accept her previous trust determination. (correct answer)

- ○ E.O. 13488 limits Miranda's mobility in transferring between agencies.
- ○ E.O. 13488 requires Miranda to undergo a new investigation.
- ○ E.O. 13488 limits which parts of Miranda's record are stored in Scattered Castles.

Feedback: *According to E.O. 13488, Miranda's new agency must reciprocally accept Miranda's previous trust determination.*

Knowledge Check 4

Zay is transferring from a cleared position with Army Medical Research to a task force dealing with biological weapons. He is denied an upgraded security clearance, and he believes it is retaliation for a lawful whistleblower complaint he made in a previous position. How does SEAD 9 apply to his case?

- ○ SEAD 9 states that denials of security clearance are final, regardless of the reason.
- ⊙ SEAD 9 establishes a process to appeal the decision. (correct answer)
- ○ SEAD 9 prohibits any appeal for positions involving weapons of mass destruction.
- ○ SEAD 9 gives Zay a right to review his investigation file for evidence of retaliation.

Feedback: *SEAD 9 establishes an appeal process for lawful whistleblowers who believe they are subject to retaliation.*

Knowledge Check 5

According to Clifford vs. Shoultz, because a background investigation is not a trial:

- ○ Adjudicators must prove an individual is a risk to national security.
- ○ Individuals are not required to swear that their responses are true.
- ○ Agencies are not required to maintain strict records.
- ⊙ Individuals may be denied security clearance for their refusal to answer questions. (correct answer)

Feedback: *According to Clifford vs. Shoultz, refusal to answer questions is grounds for an unfavorable trust determination.*

Knowledge Check 6

What is one way the FPV program has changed in response to events like the OPM Data breaches?

- ○ Individuals must be given an opportunity to appeal a denial of security clearance.
- ○ Security clearance may only be denied when it is consistent with the national interest.
- ⦿ DCSA was created to oversee personnel vetting, and new policies to promote information security were introduced. (correct answer)
- ○ The FPV program has not changed in response to these events.

Feedback: *DCSA was created in response to these attacks on the Federal workforce, and new protections were put into place.*

Lesson 3 Review Activities

Knowledge Check 1

Which of the following statements correctly describes the Federal Personnel Vetting Core Doctrine?

- ⦿ This document provides the philosophy for and guides all FPV policy. (correct answer)
- ○ This document defines intended outcomes for the FPV program, including investigations, adjudications, and PV management.
- ○ This document provides specific procedures for background investigations.

Feedback: *The Core Doctrine provides the philosophy for and guides all FPV policy.*

Knowledge Check 2

Which of the following statements correctly describes the Federal Personnel Vetting Guidelines?

- ○ This document provides the philosophy for and guides all FPV policy.
- ⦿ This document defines intended outcomes for the FPV program, including investigations, adjudications, and PV management. (correct answer)
- ○ This document provides specific procedures for background investigations.

Feedback: *The FPV Guidelines define the intended outcomes and apply key principles of the FPV Core Doctrine.*

Knowledge Check 3

Which of the following statements correctly describes the Federal Personnel Vetting Investigative Standards?

- ○ This document provides the philosophy for and guides all FPV policy.
- ○ This document defines intended outcomes for the FPV program, including investigations, adjudications, and PV management.
- ⊙ This document provides specific procedures for background investigations. (correct answer)

Feedback: *The Investigative Standards provide specific guidance for collecting background information.*

Lesson 4 Review Activities

Knowledge Check 1

The new team will hire an Information Systems Manager who requires Top Secret eligibility and access. Determining whether the individual has the trustworthiness to meet that requirement falls under which domain?

- ○ Suitability
- ○ Fitness
- ⊙ National Security (correct answer)
- ○ Credentialing

Feedback: *Decisions about access to classified information fall under National Security Eligibility.*

Knowledge Check 2

The new team will hire a Program Analyst, who will be a Federal employee. Determining whether the individual has the character and conduct necessary for that position falls under which domain?

- ⊙ Suitability (correct answer)
- ○ Fitness
- ○ National Security
- ○ Credentialing

Feedback: *Decisions about a person's character relating to the requirements of a Federal position fall under Suitability.*

Knowledge Check 3

The new team will hire an Administrative Assistant to support the daily activity of the office. Determining whether the individual is a risk to Federal facilities and information systems falls under which domain?

- ○ Suitability
- ○ Fitness
- ○ National Security
- ⦿ Credentialing (correct answer)

Feedback: *Decisions about a person's potential risk to Federal facilities and information systems fall under Credentialing.*

Knowledge Check 4

Norris has received a promotion from Project Analyst, a Low Tier position, to Project Manager, where he will require national security eligibility at the Secret level, which requires a Moderate Tier investigation. What scenario does this fall under?

- ○ Initial Vetting
- ○ Continuous Vetting
- ⦿ Upgrades (correct answer)
- ○ Transfer of Trust
- ○ Re-establishment of Trust

Feedback: *Because Norris is moving from a Low Tier position to a Moderate Tier position, this is an Upgrade.*

Knowledge Check 5

Jonathan previously had access to Secret information, before leaving the Federal workforce to care for a sick family member. He is now returning to a national security position with the same investigative tier. What scenario does this fall under?

- ○ Initial Vetting
- ○ Continuous Vetting
- ○ Upgrades
- ○ Transfer of Trust
- ⦿ Re-establishment of Trust (correct answer)

Feedback: *Because Jonathan has spent time without active security clearance, he requires a Re-establishment of Trust.*

Knowledge Check 6

Rosemary is a cleared contractor employee with access to Top Secret information. She is being vetted for a Federal position with the same level of access. What scenario does this fall under?

- ○ Initial Vetting
- ○ Continuous Vetting
- ○ Upgrades
- ⦿ Transfer of Trust (correct answer)
- ○ Re-establishment of Trust

Feedback: *Because Rosemary already has active security clearance and doesn't require an upgrade, her new agency must reciprocally accept her national security determination.*

Knowledge Check 7

Cosa received his Initial Vetting last year, and now receives periodic and automated checks. What scenario does this fall under?

- ○ Initial Vetting
- ⦿ Continuous Vetting (correct answer)
- ○ Upgrades
- ○ Transfer of Trust
- ○ Re-establishment of Trust

Feedback: *As long as Cosa maintains his security clearance, he will be enrolled in Continuous Vetting.*

Knowledge Check 8

Stephanie is an engineer who is being vetted for her first Federal contractor position. She has not worked for or on behalf of the Federal government before. What scenario does this fall under?

- ⦿ Initial Vetting (correct answer)
- ○ Continuous Vetting
- ○ Upgrades
- ○ Transfer of Trust
- ○ Re-establishment of Trust

Feedback: *Since this is Stephanie's first time being vetted, she will receive her Initial Vetting.*

Knowledge Check 9

The new office will require a software developer who will need Secret eligibility for access to automated systems containing servicemembers' publicly identifiable information. What position designation is required for this position?

- ○ Non-Sensitive
- ⦿ Non-Critical Sensitive (correct answer)
- ○ Critical-Sensitive
- ○ Special-Sensitive

Feedback: *A position requiring Secret eligibility for access to automated systems containing servicemembers' personally identifiable information would be a Non-Critical Sensitive position.*

Knowledge Check 10

The new office will require an intelligence analyst with eligibility for access to Top Secret information. The position is considered to have the potential for grave but not inestimable damage to national security. What sensitivity level is required for this position?

- ○ Non-Sensitive
- ○ Non-Critical Sensitive
- ⦿ Critical-Sensitive (correct answer)
- ○ Special-Sensitive

Feedback: *A position requiring eligibility for access to Top Secret information with the potential for grave damage to national security would be a Critical-Sensitive position.*

Knowledge Check 11

The office will hire a Technical Analyst who will require access to Secret information. What tier of investigation does this fall under?

- ○ Low Tier
- ⦿ Moderate Tier (correct answer)
- ○ High Tier

Feedback: *With access to Secret information, this is a Non-Critical Sensitive position, which are Moderate Tier.*

Knowledge Check 12

The office will hire a maintenance worker who only needs a credential to enter the building. What investigative tier does this fall under?

- ⦿ Low Tier (correct answer)
- ○ Moderate Tier
- ○ High Tier

Feedback: *Without access to classified information or duties posing a risk to national security, this is a Non-Sensitive position requiring a Low Tier investigation.*

Lesson 5 Review Activities

Knowledge Check 1

Which of these organizations is the primary ISP for the Federal Government, conducting background investigations, to include those used for national security determinations for DOD and other Federal agencies?

- ○ Office of Personnel Management (OPM)
- ○ Department of Transportation (DOT)
- ○ Department of Justice (DOJ)
- ⦿ Defense Counterintelligence and Security Agency (DCSA) (correct answer)

Feedback: *DCSA is the primary ISP for the Federal Government.*

Knowledge Check 2

A DCSA investigator uncovers a detail in an individual's work history that prompts the overall case seriousness to Major. The investigator completes the investigation and documents an alert for the adjudicator. Which Appendix provides this guidance?

- ○ Appendix A: FPV Information Types and Categories
- ○ Appendix E: Transfer of Trust Coverage Requirements
- ⦿ Appendix G: Issue and Case Seriousness Categorization (correct answer)
- ○ Appendix I: Investigative Triggers Required Actions

Feedback: *Appendix G addresses processes for case seriousness categorization.*

Knowledge Check 3

(CUI) Samantha currently holds a Moderate Tier position in the DOD. An annual check of her credit status reveals troubling financial concerns. Which Appendix describes this process?

- ○ Appendix A: FPV Information Types and Categories
- ⊙ Appendix C: Continuous Vetting Coverage Requirements (correct answer)
- ○ Appendix D: Upgrades Coverage Requirements
- ○ Appendix H: FPV Investigative Methodologies

Feedback: *Current insiders are enrolled in Continuous Vetting and subject to automated and periodic checks like this one.*

Knowledge Check 4

ISPs must ensure that background investigations cover all 16 types of information needed to make a determination of whether an individual can be a trusted insider. Which Appendix provides this guidance?

- ⊙ Appendix A: FPV Information Types and Categories (correct answer)
- ○ Appendix B: Initial Vetting Coverage Requirements
- ○ Appendix G: Issue and Case Seriousness Categorization
- ○ Appendix H: FPV Investigative Methodologies

Feedback: *The FPV information categories are listed in Appendix A.*

Knowledge Check 5

Matthew is a Federal employee with access to Top Secret information. He has accepted a position as a contractor with the same level of access. Which Appendix describes this vetting scenario?

- ○ Appendix B: Initial Vetting Coverage Requirements
- ○ Appendix D: Upgrades Coverage Requirements
- ⊙ Appendix E: Transfer of Trust Coverage Requirements (correct answer)
- ○ Appendix F: Re-establishment of Trust Coverage Requirements

Feedback: *A Federal employee becoming a contractor would be vetted under the Transfer of Trust scenario.*

Lesson 6 Review Activities

Knowledge Check 1

Which of the following are defined in the Common Principles in Applying Federal Personnel Vetting Adjudicative Standards?

- ☑ The Order of Operations for trust determinations (correct answer)
- ☐ HSPD-12 Credentialing standards
- ☐ Federal Personnel Vetting Guidelines
- ☑ Guidelines for preliminary trust determinations (correct answer)

Feedback: *The Common Standards provide the Order of Operations for trust determinations, and guidelines for preliminary trust determinations.*

Knowledge Check 2

Which of the following are defined in the Common Principles in Applying Federal Personnel Vetting Adjudicative Standards?

- ☐ Position designation categories
- ☐ Appeal processes for legal whistleblowers
- ☑ Guidance for risk assessment (correct answer)
- ☑ Adjudicative Process Framework (correct answer)

Feedback: *The Common Standards provide the Order of Operations for trust determinations, and guidelines for preliminary trust determinations.*

Knowledge Check 3

Liqiao is a naturalized U.S. citizen being vetted for national security eligibility. Which of the following statements is true about the adjudication process for Liqiao?

- ○ The adjudication will not consider events that took place before Liqiao immigrated to the United States from China.
- ⊙ All available, reliable evidence about Liqiao should be considered to make a determination, no differently from other cases. (correct answer)
- ○ Adjudicators will use guidelines specialized for Chinese-American citizens to evaluate Liqiao's case.
- ○ Liqiao's political and cultural activities must be given greater weight than those of native-born citizens.

Feedback: *Liqiao will be vetted with the same thoroughness as any other individual. This is called the Whole Person Concept.*

Knowledge Check 4

Noelle Kirkpatrick is being vetted for a position handling Secret Information. During her Initial Vetting for National Security Eligibility, the adjudicator finds that four years ago, she was terminated from a position while managing an opioid use disorder. Which of the following must the adjudicator consider as they review her record?

- ☑ Whether the substance misuse occurred after a severe or prolonged illness or injury (correct answer)
- ☐ How many other candidates for the position have shown the same conduct
- ☑ The presence or absence of rehabilitation and other permanent behavior changes (correct answer)
- ☐ Not applicable; the adjudicator must make an unfavorable determination when opioid misuse is involved.

Feedback: *The adjudicator will consider circumstances like Noelle's medical history and attempts at rehabilitation.*

Knowledge Check 5

Joseph Kim is being vetted for Suitability for a High-Risk position. Which of the following factors must be considered from 5 CFR Part 731?

- ☑ Material, intentional false statement (correct answer)
- ☑ Misconduct or negligence in employment (correct answer)
- ☐ Political or religious affiliation
- ☐ Educational attainment

Feedback: *Material, intentional false statement and misconduct or negligence in employment are both factors from Part 731.*

Knowledge Check 6

Leonard Navarro is currently a trusted insider with access to Top Secret information. As part of his Continuous Vetting, the adjudicator is evaluating Leonard's current difficulties meeting financial obligations. Which of the following must the adjudicator consider?

- ☐ Whether Leonard performs volunteer or charity work in the community
- ☑ Whether Leonard has self-reported the information.
- ☑ Whether Leonard has sought professional financial assistance to resolve his debt (correct answer)

- ☑ Whether Leonard is demonstrating positive changes in financial behavior (correct answer)

Feedback: *The adjudicator would consider whether Leonard self-reported the information, whether he has sought assistance, and whether he has changed his behaviors.*

Knowledge Check 7

Chelsea Shaw is being vetted for her Suitability for a Moderate-Risk position. Which of the following issues indicate factors that must be considered from 5 CFR Part 731?

- ☑ Chelsea did not report that she was terminated from a previous position for cause. (correct answer)
- ☐ Chelsea was a member of a sorority in college.
- ☑ Ten years ago, Chelsea had a restraining order placed against her by an ex-partner. (correct answer)
- ☐ Chelsea does not drink alcohol.

Feedback: *Chelsea's termination and restraining order would both fall under factors described by 5 CFR Part 731.*

Knowledge Check 8

Catalina Morales is being vetted for Credentialing for access to a Federal worksite. Which of the following information could disqualify Catalina from receiving a credential?

- ☑ There is a reasonable basis to believe Catalina will use a credential outside the workplace inappropriately. (correct answer)
- ☐ Catalina has never been charged with a crime.
- ☑ Catalina does not meet the agency's supplementary credentialing standards. (correct answer)
- ☐ Catalina was injured in an auto accident seven months ago.

Feedback: *Concerns about Catalina's use of the credential and her failure to meet supplementary standards could both disqualify her from receiving a CAC.*

Knowledge Check 9

Ruth is a DOD Paralegal Specialist with eligibility and access to Secret information. She will require temporary access to Top Secret information while working a court

case that is expected to last nine months. Which of the following must be accomplished for her to obtain access?

- ☑ Favorable review of SF 86 (correct answer)
- ☑ Citizenship verification (correct answer)
- ☑ Favorable review of FBI and NCIC law enforcement checks (correct answer)
- ☑ Initiation of an expedited investigation (correct answer)

Feedback: *All of these must be accomplished for Ruth to gain temporary access.*

Knowledge Check 10

Jude is receiving his Initial Vetting for a Federal position, and the agency head is considering authorizing a preliminary trust determination. Which of the following are true?

- ☑ The preliminary determination must be based on information from high-yield checks. (correct answer)
- ☐ Jude must receive a favorable Credentialing determination before preliminary access can be authorized.
- ☐ The agency must receive Executive Agent permission to authorize a preliminary determination.
- ☑ The agency head may authorize security personnel to make the determination. (correct answer)

Feedback: *The preliminary determination is based on the results of high-yield checks, and the agency head may authorize security personnel to make the determination.*

Lesson 7 Review Activities

Knowledge Check 1

Benjamin is undergoing Initial Vetting for Top Secret eligibility and access. Which of the following actions correctly apply the requirements to safeguard personnel vetting information?

- ☑ The background investigator reviews the gathered information to verify that it is relevant and timely. (correct answer)
- ☑ The adjudicator making the determination is properly trained in information security. (correct answer)
- ☐ The adjudicator deletes information from Benjamin’s file that they do not believe is relevant.

- ☐ The background investigator provides Benjamin with several records from his personnel vetting file.

Feedback: *The Background Investigator and Adjudicator must ensure information is relevant and timely, and they must be properly trained in information security.*

Knowledge Check 2

Annie is transferring to a new Federal position with the same level of risk and access as her current position. Which of the following information must be documented in her FPV record?

- ☑ The reciprocal acceptance of Annie's previous trust determinations (correct answer)
- ☑ Any exceptions that may apply to Annie's national security eligibility (correct answer)
- ☑ The date Annie's polygraph examination takes place (correct answer)
- ☐ Any information that is withheld from the database for national security purposes

Feedback: *The adjudicator must document Annie's reciprocal acceptance, exceptions, and polygraph information.*

Knowledge Check 3

Connie is being vetted for an Upgrade to Top Secret eligibility and access. Which of the following actions correctly apply the requirements to safeguard personnel vetting information?

- ☐ The adjudicator discusses information collection methods over unsecured media.
- ☑ The information collection process is not unduly intrusive. (correct answer)
- ☑ The adjudicator uses a risk-based approach to identify vulnerabilities and threats. (correct answer)
- ☑ Information sharing between agencies makes the process more efficient. (correct answer)

Feedback: *Information collection must not be unduly intrusive, must use a risk-based approach, and should maximize efficiencies through cooperation with other agencies.*